CHAPTER

5

DESIGNING A MULTI-PROTOCOL STRATEGY

After reading this chapter and completing the exercises, you will be able to:

- Design a strategy to integrate NetWare in a Windows 2000 environment
- Design a method to access IBM mini and mainframe systems with Windows 2000
- Design a connection solution between Windows 2000 and UNIX hosts
- Design a mechanism for Macintosh systems to access Windows 2000 systems

Many, if not most, networks contain a mixture of operating systems and services. Sometimes you'll want to replace these systems with Windows 2000 services; in other cases, integrating with existing non-Windows 2000 systems is a better solution. In this chapter, you are shown strategies for integrating Windows 2000 with other operating systems, and you discover how to access and integrate with NetWare, IBM, UNIX, and Macintosh systems.

Designing Connectivity to NetWare Resources

Services hosted by NetWare systems have been around for several years and are used today in many networks. Windows 2000 services and protocols allow you to access information and use resources managed by NetWare services without the need to migrate the information and resources to Windows 2000 systems. In addition, you can migrate account information and files from NetWare systems to Windows 2000. This feature allows you to transition all or some of your NetWare services to Windows 2000. In the following sections, we discuss the protocols and services related to NetWare resources and the NetWare integration designs you can create and enhance.

Protocols

Until recently, NetWare servers and services used only the **Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX)** protocol for communications between clients and servers. This protocol was developed by Novell and is necessary for proper communications between NetWare 2.*x*, 3.*x*, and 4.*x* servers. NetWare 5.*x* servers can use **Transmission Control Protocol/Internet Protocol (TCP/IP)** or IPX/SPX for communications.

IPX/SPX is an optional protocol for NetWare 5.*x* servers, but many NetWare 5.*x* servers use IPX/SPX because other services or clients on the network are dependent on IPX/SPX. Microsoft provides a 32-bit implementation of IPX/SPX in Windows 2000 called **NWLink**. NWLink is an IPX/SPX/NetBIOS-compatible transport protocol. You must use this protocol if you plan on using the NetWare services included with Windows 2000. If you have NetWare 5.*x* servers that are using only TCP/IP, you will need to enable IPX/SPX on those NetWare 5.*x* servers.

NWLink is a self-configuring protocol—it does not need to be configured. When a system using NWLink starts up, the system monitors network traffic and uses the IPX/SPX parameters it detects to configure NWLink. If needed, or preferred, you do have the ability to manually assign the IPX/SPX values to NWLink. The process of automatically detecting the IPX/SPX parameters generates additional traffic on the transmission media. When a Windows system that is configured to auto-detect IPX/SPX parameters starts up, it broadcasts packets to determine the frame type used for IPX/SPX. These broadcast packets reach each device on a hub-based or switched Ethernet network.

Imagine the traffic generated on a network when many users power up their machines in the morning or at the beginning of a shift period. This is no time for your coffee break! To reduce the amount of traffic, you can specify the IPX network number for the Ethernet frame type used by the NetWare systems. This is configured in the properties of the NWLink IPX/SPX/NetBIOS Compatible Transport Protocol dialog box that you can access through Local Area Connections. The default configuration is auto frame type detection. To specify the IPX/SPX parameters, enable manual frame type detection, as shown in Figure 5-1.

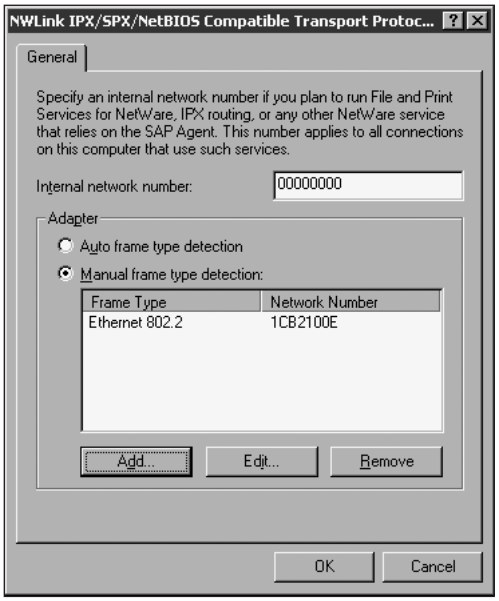

Figure 5-1 NWLink IPX/SPX/NetBIOS Compatible Transport Protocol dialog box

The next step is to specify the frame type and the network number. If you do not know the proper values used on the network, contact the NetWare administrator to obtain them. If the frame type and/or network number(s) is/are not correct, the NetWare services provided by Microsoft will not be able to communicate with the NetWare resources.

When you enable the manual frame type, the Add button in the NWLink IPX/SPX/NetBIOS Compatible Transport Protocol dialog box is enabled. To set the frame type and its associated network number, click the Add button and fill in the appropriate information. In Figure 5-1, the frame type used by the NetWare systems is Ethernet 802.2 and the corresponding IPX/SPX network number is 1CB2100E. If you forget to specify at least one frame type and network number, the Windows system uses auto frame type until you set the manual frame type values.

Microsoft provides two strategies for accessing NetWare services from Windows 2000. One solution uses a **gateway** service running on a Windows 2000 server. This method permits other Windows systems—such as Windows 95/98, NT, and 2000—access to the NetWare resource without the need to install additional software on each Windows system. The second method uses installed software on each Windows machine that needs access to the NetWare resources. The software installed on each Windows 2000 machine is called **Client Services for NetWare (CSNW)**. Both methods allow you to use NetWare file, print, and directory services. These NetWare services might be housed on **bindery** servers (NetWare 3.*x*) or on **Novell Directory Services (NDS)** servers (NetWare 4.*x* and higher).

NetWare 3.*x* servers use a local database called the bindery to store all the user account information. When two or more NetWare 3.*x* servers are present and a user needs to access resources managed by each server, an account must exist for the user in each of the NetWare 3.*x* servers' binderies. In a bindery-based environment, you can specify the preferred server to log into. This setting is specified through properties of the software elements involved. If this is not specified, the user's machine will discover an available server and use that to access the network.

In the early 1990s Novell introduced NDS, an X.500-based directory service that stores all the account and resource information in a network-wide database. NDS can be partitioned and replicated among different NetWare 4.*x* and/or 5.*x* servers to provide access to authentication and management services; it also provides fault tolerance.

In an NDS environment, the users log into the database, which is often referred to as the tree. The name tree comes from the hierarchical structure of the NDS database. NDS uses objects, called containers, to organize users and objects in the database for security and management purposes. When a user in an NDS network needs to log into the database, both the name of the tree and the location or context of the user object in the tree must be specified. These values are set through properties of the software elements involved.

Services

Microsoft provides several solutions and products—or services—for Windows 2000 to access and/or manage NetWare network resources. If the existing network is primarily Windows operating systems or the organization plans to migrate to Windows systems, services such as Gateway Services for NetWare or Client Services for NetWare are probably good options. Some of the other options, such as File and Print Service for NetWare, are better suited for environments that use primarily NetWare operating systems and have a few Windows 2000 systems.

The following several sections describe each of the services Microsoft provides for working with NetWare networks. We also mention the type of environment for which each service is best suited.

Gateway Services for NetWare

Gateway Services for NetWare (GSNW) is installed on a Windows 2000 server system. It will not run on Windows 2000 Professional. The Windows 2000 server machine acting as the gateway must have NWLink installed. The installation process for the gateway services will automatically install NWLink if it is not already present.

The Gateway Services for NetWare running on a Windows 2000 server provides a portal or gateway between Windows machines and NetWare file and print services. Whenever a Windows system requests access to a NetWare resource, all requests are funneled from the Windows systems through the GSNW service to the NetWare information.

Examples of NetWare-managed resources that users may need to access include printers and shared files. As an example of the use of this service, imagine a mixed NetWare and Microsoft network in which some of the shared data files are stored on a NetWare server. In this example, GSNW would allow users access to the Windows 2000 network and access the files on the NetWare server.

Resources managed by NetWare require the use of accounts, passwords, and other security parameters to control access. An account must exist in the NetWare system to allow gateway services access to the NetWare resources. Each Windows machine using Gateway Services for NetWare uses the same NetWare account to gain access to the NetWare resources. Therefore, you must use or create a new NetWare user account that provides the appropriate access to the necessary NetWare resources for all your Windows-based machines that use the gateway. Figure 5-2 diagrams the flow of information between Windows clients, GSNW, and the NetWare resources.

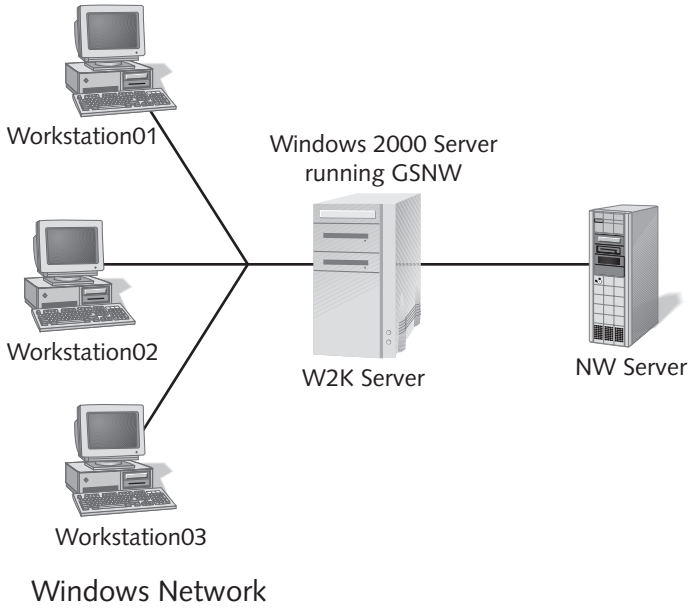

Figure 5-2 Gateway Services for NetWare information flow

In Figure 5-2, when a user working on the Windows system labeled Workstation01 needs access to resources on the NetWare server titled NW Server, all requests and responses go through the gateway service running on the Windows 2000 server labeled W2K Server. The NetWare resource request from Workstation 01 travels to W2K Server. The GSNW on W2K Server sends the request to NW Server using the account and password specified in the GSNW service properties. When the request is fulfilled by the NetWare server, any responses due back to the requester (Workstation01) are delivered to W2K Server. The W2K Server then sends the response to Workstation01.

The same process occurs for all the Windows machines requesting access to a NetWare resource. The Windows 2000 server also can gain access to NetWare resources by using the GSNW services it is running. Notice that as the number of Windows machines using the gateway increases, a bottleneck develops at the GSNW machine. It is for this reason that GSNW is recommended only for occasional access to NetWare resources. If you need frequent access to NetWare resources, install additional gateway systems, use Client Services for NetWare, or install Novell Client for Windows NT/2000.

Novell Client for Windows NT/2000 is a Novell product and can be downloaded free from the company's Web site (*www.novell.com*). If you are using other versions of Windows, such as Windows 95/98, Novell provides clients for all versions of Windows and these also can be downloaded for no charge from Novell's Web site.

Gateway Services for NetWare requires a NetWare group and a user account that is a member of the group. The NetWare group required is a standard NetWare group and the name must be **NTGATEWAY** (case is not important). The NetWare user account that will be used to pass all requests to and from NetWare services must be a member of the NTGATEWAY group. You will receive an error message if the group and user account membership are not set up when you attempt to configure the gateway following GSNW installation. Without the NetWare group and user account membership, you will not be able to use the gateway services.

Installing and configuring GSNW is a multi-step process. The basic outline of the steps is:

1. Install GSNW on a Windows 2000 server
2. Log into the NetWare service from the Windows 2000 server
3. Reboot the Windows 2000 server
4. Enable the gateway on the Windows 2000 server
5. Specify the NetWare account and password information in the GSNW program

To install and configure GSNW on a Windows 2000 server, you must be the administrator or a user that is a member of the Administrators group.

NetWare user account passwords are *not* case sensitive. However, they are spelling sensitive!

Gateway Services for NetWare is installed as a network client service through Local Area Connection Properties. Using the Install button in the Local Area Connection Properties window brings up the Select Network Component Type selection window. There are three categories of components available: Client, Service, and Protocol. GSNW is classified as a Client component. When you choose Client, your system will

take a few moments to detect what is already installed and what is available. Figure 5-3 shows the Select Network Client window that is displayed when your system has completed its self-evaluation. For GSNW, select Gateway (and Client) Services for NetWare, and click the OK button.

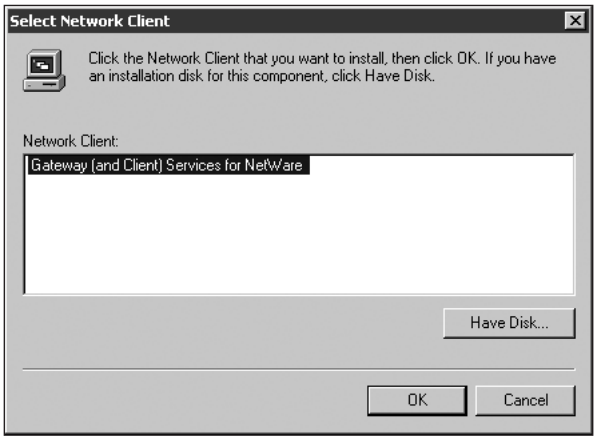

Figure 5-3 Selecting the GSNW component for installation on a Windows 2000 server

During the finishing stages of installing the GSNW service, a dialog box appears, requesting the name of the NetWare server for bindery-based systems or the name of the tree and context for NDS-based systems. You also have the option to run or not run the Novell login scripts. After you complete the necessary login steps, the installation process will prompt you to reboot your system. NetWare **login scripts** contain commands to be executed when the user logs into the NetWare environment. The commands may consist of drive map specifications or printer assignments. Login scripts are a convenient mechanism to specify the same settings and environment for multiple users.

After your system has rebooted, you need to configure and enable the gateway services. The GSNW management interface is installed as a Control Panel component. The Gateway button on the GSNW window opens another window for configuring the name and password of the NetWare account that GSNW will use to communicate with the NetWare system. Remember, the NetWare account you specify here must be a member of the NTGATEWAY NetWare group.

Any NetWare rights assigned using the user account specified in the gateway settings apply to all users using the GSNW service. Similarly, any NetWare rights assigned using the NTGATEWAY group apply to all users using the GSNW.

As an example of how this works, let's say that the name of the gateway NetWare account is GSNWUser. In addition, on the NetWare server, the user account GSNWUser is assigned the Read, Write, Create, Erase, Modify, and File Scan rights to

the Correspondence directory. Therefore, every Windows user that uses the gateway service to access the NetWare network will have the Read, Write, Create, Erase, Modify, and File Scan rights on the Correspondence directory.

The Configure Gateway window allows you to create named shares and drive letters for NetWare resources. If you choose not to run the NetWare login scripts, setting up shares in the Configure Gateway interface gives all Windows users of GSNW the same names and drive letters for NetWare resources. In addition, the shares defined in GSNW appear as Windows shares to users accessing resources on the Windows 2000 server running the GSNW software.

The Gateway Service for NetWare configuration window also has print and login script options. If you choose to run the NetWare scripts when a Windows user connects to the gateway service, check the Run Login Script check box. The print options include the ability to do the following:

- Print the document as is or add a form feed at the end of the document
- Notify the user when the document is printed
- Specify the absence or presence of a banner page**.** A banner page prints at the beginning of the document and identifies who printed the document. Banner pages are useful when there are many different users printing at the same time and can help separate the individual print jobs.

The Windows 2000 server that is running the GSNW service also can access the NetWare resources. It is essentially running Client Services for NetWare, although it is not listed as a separate service. When you log on to a Windows 2000 server running GSNW, the system will attempt to authenticate you to the NetWare system using the Windows 2000 account and password you entered. If either the account and/or password does not match an account and/or password in NetWare, a dialog box appears requesting the name and/or password of a valid NetWare account.

The NetWare user account used when logging on to the Windows 2000 server running GSNW and NetWare does not have to be the same NetWare account used by the GSNW service. In addition, the NetWare user account specified when logging on to Windows 2000 does not have to be a member of the NTGATEWAY NetWare group.

Client Services for NetWare

Client Services for NetWare (CSNW) is designed for environments that access NetWare resources frequently and that plan to retain the NetWare resources. In contrast to the gateway services, CSNW is installed on each Windows 2000 Professional machine that needs access to NetWare resources. Because a single gateway is not used, each Windows 2000 user can use a different NetWare account.

To appreciate the uses of CSNW, imagine a directory titled Templates that resides on a NetWare server. Some users need to modify the documents while other users only need to read the documents. Under the NetWare security system, you can assign the Read, Write, Modify, and File Scan rights to the users who need to modify the documents. For the other users, assigning the Read and File Scan rights would allow those users the ability to read the files but not make changes to the documents. This provides more flexibility on securing NetWare resource access, but does require management of user accounts in the NetWare network.

CSNW software is installed as a client service through the properties of the Connection object in Network and Dial-up Connections. To install CSNW, the Windows 2000 account that is logged on must be the administrator or a member of the Administrators group. In addition, CSNW requires NWLink and, if this is not already present, the CSNW installation program will install NWLink automatically.

During the installation process, you specify in the Select NetWare Logon window the name of the NetWare server for bindery-based NetWare networks or the name of the **tree** and **context** for NDS-based NetWare networks. The tree is the name of the NDS database and the context is the location of the user object in NDS. You also can specify if you want the NetWare login scripts to run when the user logs into the NetWare environment. When the information in the Select NetWare Login screen is entered, you will be prompted to reboot your computer.

When you log on to a Windows 2000 machine running the CSNW software, the software uses the Windows 2000 user account and password and attempts to find a match for the same items in the NetWare environment. If the account name and passwords match, there is no prompt for NetWare user name and password. If the account name matches but the passwords do not, the Enter Password window appears requesting the password for the NetWare user account. If there is no matching NetWare account when you log on to Windows 2000, the Select NetWare Logon window appears. Because there is no matching NetWare user account of the same name as the Windows 2000 user account, you will not be able to log into the NetWare network.

Configuration of the CSNW software is accessed through a Control Panel applet titled CSNW. When the CSNW Control Panel applet is opened, the Client Services for NetWare window is presented. This window allows you to change the name of the server for bindery-based NetWare systems and the name of the tree and context for NDS-based NetWare environments. You also can opt to run the NetWare login scripts and specify printing options such as form feed, printing notification, and banner pages.

Services for NetWare v.5

Microsoft provides additional NetWare interoperability tools bundled as a separate product called **Services for NetWare (SFN) v.5**. These are designed for integrating Windows 2000 server systems into an existing NetWare environment. There are two products contained in the SFN package: Microsoft Directory Synchronization Services (MSDSS) and File and Print Services for NetWare (FPNW). Services for NetWare v.5

is a separate product and is not included on the standard Windows 2000 Advanced and Windows 2000 Server installation CDs.

We next discuss each of the two products contained in the SFN package.

Microsoft Directory Synchronization Services

Microsoft Directory Synchronization Services (MSDSS) is designed for mixed Windows 2000 and NetWare networks that need to retain services operating on both environments. MSDSS synchronizes information between Microsoft's **Active Directory** (**AD**) and NDS, providing one-way or two-way synchronization of data between AD and NDS and making management of two separate directory services easier.

If the majority of your account and group management is handled through Windows 2000, MSDSS can be configured for one-way synchronization. With one-way synchronization, changes made in the Windows 2000 AD environment are synchronized to NDS but changes made in NDS are not synchronized to AD.

As an example of the use of MSDSS, consider an employee who has changed departments and the description property in her user accounts needs to be changed. With one-way synchronization set up, you can make the change in Windows to the user's description property and MSDSS will send that change to NDS and modify the user's description property in NDS.

MSDSS also can be configured to migrate user accounts and groups from NDS to AD. This allows networks that plan on removing or reducing their NetWare network the ability to copy existing information into Windows 2000 AD instead of reentering the information.

MSDSS requires Novell Client for Windows NT/2000. It modifies the initial Windows 2000 logon screen, but it allows you to log on to Windows 2000 and NDS or just to Windows 2000. Novell Client and Gateway Services for NetWare cannot coexist on the same Windows 2000 server. If you need to maintain the GSNW services and use the directory synchronization services, the MSDSS and GSNW products will need to be installed on different Windows 2000 servers.

The MSDSS software must be installed on a domain controller and the account logged on to Windows 2000 Advanced Server, or Windows 2000 Server must be the administrator or an account that is a member of the Administrators group. In addition, you will need to know the name and password of the NetWare account that has full rights to NDS.

Installation of MSDSS is initiated by launching the MSDSS.MSI file located on the Services for NetWare v.5 CD. The installation process includes two setup types: Typical and Custom. Typical is self-explanatory for anyone who has ever installed any piece of Microsoft software, and Custom allows you to specify whether you want to synchronize passwords between AD and NDS and to install the Management Console snap-in and the Help files. During installation, a dialog box appears requesting confirmation to update the Active Directory schema for directory synchronization. The schema defines the types of objects, their properties, and the placement of the objects in the directory

services structure. Because NDS and AD use different schema definitions, there needs to be some modification of the AD schema to accommodate proper information synchronization between AD and NDS. If you choose not to update the AD schema, the installation of MSDSS is cancelled.

After MSDSS is installed, three additional menu items are added to the Administrative Tools menu: Directory Synchronization, Microsoft File Migration utility, and MSDSS Backup & Restore utility. Directory Synchronization allows you to connect or map information between AD containers and NDS containers. The Microsoft File Migration utility allows you to migrate a copy of existing files on NetWare servers to Windows 2000 systems. The MSDSS Backup & Restore utility is used to back up the mapping information that exists between AD and NDS objects.

When you first open the Directory Synchronization tool following MSDSS installation, there are no connections between AD and NDS. For each container in AD that you wish to synchronize to a container in NDS, a **session** must be configured. A session is a logical connection between Active Directory and Novell Directory Services. This connection provides a delivery path for the information to be synchronized between the two different databases. Since both AD and NDS are structured hierarchically and use containers to organize users and resources, each container in AD that you want to synchronize with NDS must be configured as separate sessions. In addition, for each session, you specify if it is a one-way synchronization, a two-way synchronization, or a migration of the information from NDS to AD.

Microsoft uses the terms **publisher** and **subscriber** to indicate the direction of information flow. The publisher is Active Directory and the subscriber is NetWare. As an example of these roles, assume there is an organization unit (a container) in Active Directory called Austin. Inside this container are user accounts and a few groups. In NDS, there is also an organization unit of the same name, Austin, that contains user accounts and groups for the same group of people in AD. If you want to synchronize changes between the two databases, you set up a session between the Austin container in AD and the Austin container in NDS. In this scenario, the publisher is the Austin container in AD and the subscriber is the Austin container in NDS. Figure 5-4 shows a completed session between the two different databases.

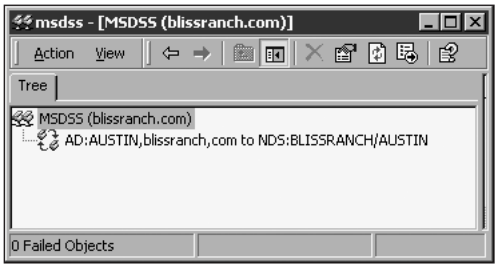

Figure 5-4 Synchronization session between AD and NDS

The name of the session in Figure 5-4 is the default name created by the synchronization tool. In this example, AD:AUSTIN,blissranch,com refers to the publisher and NDS:BLISSRANCH/AUSTIN refers to the subscriber. When you create a session, you can use a different name than the default name.

A one-way synchronization is from publisher (or AD) to subscriber (or NDS). A two-way synchronization is from publisher (AD) to subscriber (NDS) and back to publisher (AD). The migration option is from subscriber (NDS) to publisher (AD). If management is primarily accomplished on the AD side, one-way synchronization is recommended. If the network plans on moving from NetWare to Windows 2000 or plans on reducing the number of NetWare services, the migration option is recommended. This allows you to copy the existing information from NDS into AD without the need to reenter all the user and group information. In addition, the migration method provides an option to migrate the files from a NetWare server to Windows 2000.

Once you decide which synchronization option you will be using, the Directory Synchronization tool prompts you for the name of the AD container, the name of the NDS container, and the name and password of an account in NDS that has full NDS rights. If you have chosen a two-way synchronization, the NDS schema will need to be extended to support two-way synchronization. To extend the NDS schema, the NDS account specified in the synchronization session must have full NDS rights to the entire NDS database (tree). If you choose not to extend the NDS schema, a one-way synchronization will be created. When all the information has been entered, the Directory Synchronization tool will perform the action you specified.

MSDSS also works with bindery-based NetWare networks.

The Microsoft File Migration utility allows you to migrate copies of files from NetWare systems to Windows 2000. There are six configuration steps that must be completed before you can migrate any files:

1. *Select the MSDSS mapping file*: If you set up a custom mapping when creating a session in the Directory Synchronization tool, this first step involves locating the MSDSS mapping file. A custom map file contains information about user accounts and group objects in NDS and how they map to or correlate to objects in Active Directory. If you did not set up a custom map, you do not specify a map file in the Microsoft File Migration utility.
2. *Select security accounts used for migration*: The name of the NDS account and password that will be used for the migration process must be specified. This NetWare account needs the proper NetWare rights to access the files that will be migrated. If you are not using a custom mapping file, the NDS and AD accounts and passwords are already specified and you cannot change

these. If you have used a custom mapping file, the values in the Select Security Accounts Used for Migration window can be modified.

3. *Select source and target volumes to migrate*: In this step, you specify the volumes and/or directories on the NetWare server that will be migrated to shares on Windows 2000. Microsoft uses the terms "source" for the NetWare resource and "target" for Windows 2000. Once you have a source and target specified, the MAP button "connects" the two resources for migration purposes. When you have specified all of the "maps," you continue to the next step.
4. *Enable logs and change logging settings*: This allows you to indicate if you want a log file created, the location of the log file, the specifications on file size, and the rollover options.
5. *Scan source and destination file volumes and shares*: The migration tool provides the ability to scan the source and target systems. This ensures that all the selected source files can be read and written to the target and that there is sufficient disk space on the Windows 2000 computer to hold the migrated files. If there are any errors, you can exit the Microsoft File Migration utility and nothing will change on the Windows 2000 side or the NetWare side.
6. *Start migration*: If there are no scanning errors and you want to proceed, the last step is to start the migration.

When you exit the Microsoft File Migration utility, you have the option to save your configuration settings so you can return to the same environment at another time.

The MSDSS Backup & Restore utility is used to back up the sessions you have set up with the Directory Synchronization tool. Each session you configure creates a session database that stores the Active Directory and NDS object mappings. Because these databases are critical for proper synchronization of objects between AD and NDS, it is important to back them up in case of file corruption.

The MSDSS Backup & Restore utility can be configured to perform automatic backups at certain times. These backup files are placed in the *systemroot*\System32\Directory Synchronization\Backup directory. The original, active session database files are stored in the *systemroot*\System32\Directory Synchronization\Data Files directory. You cannot modify the location of the backup directory and the previous backup files will be deleted automatically to accommodate the new backup files created.

File and Print Services for NetWare (FPNW)

Networks that are primarily running services on NetWare servers and are maintaining account and security functions using Novell solutions may have one or more Windows 2000 servers present. Often, software that an organization needs will run only on specific operating systems. If the software can run on a Windows 2000 server but not on a NetWare server, then a Novell network may contain Windows 2000 servers to host the needed software. In this type of environment, the users' Windows machines are most likely running Novell Client to access resources on the NetWare network.

One way to allow NetWare users access to the Windows 2000 resources is to use Client for Microsoft Networks on the users' machines. However, it is also probable that the users in a NetWare environment may not want to run Client for Microsoft Networks and are only running Novell Client to access network resources and services. In this type of environment, running **File and Print Services for NetWare** (**FPNW**) on the Windows 2000 servers is a good solution. To the users in the NetWare environment, the FPNW allows the Windows 2000 servers to appear as NetWare 3.*x* servers. No additional software is installed on the users' machines and no changes to the existing Novell Client are required.

Because FPNW emulates a NetWare 3.*x* server, NWLink must be running on the Windows 2000 server providing the FPNW service. If NWLink is not present on the Windows 2000 server, the FPNW installation process will install NWLink. In addition, the **SAP Agent** is installed on the Windows 2000 server if it is not present and is used on a Windows 2000 system to respond to queries from clients.

Service Advertising Protocol (SAP) is used by IPX/SPX-based NetWare services to "advertise" their presence and the services they provide. An IPX/SPX-based NetWare server will advertise its availability so that the Novell clients can connect and access resources. Because the Windows 2000 server running FPNW services emulates a NetWare 3.*x* server, it must also advertise its presence. This advertisement role is provided by the SAP Agent. This concept of systems "discovering" the presence of other services and/or systems is similar to the Windows 2000 browser service.

FPNW is installed as a service in the Local Area Connection properties window. For the service to function properly, a user account titled FPNW Service Account is created in the domain where FPNW is installed. If you are installing FPNW on more than one domain controller in a domain, you must enter the same password for this account when installing on the different domain controllers. The FPNW Service Account user account is automatically added to the Administrators group. Do not delete this account because it must be present for the FPNW service to start up. At the end of the FPNW installation process, you will need to reboot the Windows 2000 server.

When a Windows machine running Novell Client browses the network, the Windows 2000 server running FPNW appears as another NetWare server. The name of the Windows 2000 server running FPNW is the name of the Windows 2000 machine, followed by an underscore and fpnw. For example, if the Windows 2000 machine is W2KInventory, the name as it appears to the Novell Client machine would be W2KInventory_fpnw.

Directory Services Manager for NetWare

At the time of this writing, Directory Services Manager for NetWare could only run on Windows NT 4.0 servers. The service allows you to add NetWare servers to a Windows NT 4.0 domain. This provides a mechanism for users to maintain only one user account and password to access resources in a Windows NT 4.0 and NetWare network.

NetWare Integration Designs

In a mixed Windows and NetWare network, the frequency of access to NetWare resources is an important design element. If users are only occasionally accessing NetWare services, Gateway Services for NetWare is a good choice. However, if clients frequently access the NetWare network, then either Client Services for NetWare or Novell Client is a recommended solution. In networks where the primary service provider is NetWare and clients are already using Novell Client, running File and Print Services for NetWare is a solution.

Enhancing NetWare Integration Designs

Because Gateway Services for NetWare creates a central point through which all requests to NetWare resources pass, placement of these gateway machines in the network is important. If your organization has NetWare resources at more than one geographic location, you should place at least one GSNW Windows 2000 server in each of the branch networks. Windows 2000 systems running Client Services for NetWare and File and Print Services for NetWare should be distributed throughout the network so they are close to the clients requesting their resources.

Designing SNA Connectivity to IBM Mini and Mainframe Computers

Organizations and companies that use a centralized solution for running software and services may be using IBM mini or mainframe computers. Instead of using specialized or dedicated equipment to access the IBM systems, Windows 2000 servers can be configured to access information hosted on IBM mainframes. Microsoft's solution to integrate with IBM systems is called Microsoft SNA Server.

Microsoft SNA Server supports access to IBM mainframe, midrange, AS/400, and IBM-mainframe-compatible systems. Microsoft SNA Server is a back-office application that runs on Windows 2000 servers and acts as a gateway between IBM host systems and Windows 2000 systems.

In the following sections, we give an overview of the protocols and services surrounding SNA Server, its deployment models, and the creation and enhancement of integration designs.

Protocols and Services Surrounding SNA Server

IBM systems may use either the TCP/IP protocol or the **Systems Network Architecture (SNA)** protocol for communications. SNA is a proprietary protocol developed by IBM. In addition, non-Windows-based systems can access the IBM host services by communicating through the SNA Server gateway.

The Windows 2000 RAS service allows Windows and non-Windows clients running certain protocols to use the SNA Server gateway. This ability is important because you may have users who need to access IBM systems from non-Windows machines on UNIX, Linux, or Macintosh systems. You can set up the Windows 2000 server running SNA Server to support any or all of the following protocols:

- TCP/IP
- IPX/SPX
- NetBEUI
- Banyan VINES IP
- AppleTalk

There are two types of connections that provide the communication between Windows 2000 systems and IBM host systems. The first type is the client-to-server connection, which establishes the communication path between the Windows 2000 systems and the SNA server. These links may be either a LAN or a WAN remote access connection. The second type is the server-to-host connection and exists between the IBM host systems and the Windows 2000 SNA server.

After the SNA server is configured, Windows 2000 users can access data and applications hosted by the IBM mainframe systems. In addition, if the IBM-managed services include printing services, the clients connecting to the SNA server can use the IBM-managed printing services. For environments that use IBM systems for online transaction processing, SNA Server supports access to these services for Windows 2000 systems. SNA Server includes emulators for 3270 and 5250 for interactions with IBM mainframes and AS/400 systems, respectively.

Emulators are software programs that provide an interface that acts as if you are working on an actual terminal or console connected to the mainframe systems.

The SNA Server management interface is integrated with the Microsoft Management Console (MMC). This allows you to monitor performance and security values through the same management interface used by native Windows 2000 components.

SNA Deployment Models

Before you can introduce SNA Server into your environment, you must first choose a deployment model. A deployment model is the design and methods for the placement of your Windows 2000 and SNA systems. There are three types of deployment models to consider:

- Branch

- Centralized
- Distributed

We discuss each in turn.

Branch Deployment Model

In the **branch deployment model**, the IBM host systems are physically separated from the network users and the SNA server. This type of arrangement is common for enterprise networks that have the IBM host systems geographically centralized. Each satellite or branch office has an SNA server that communicates with the centralized IBM systems using the SNA protocol. The clients at each satellite office communicate with the local SNA server using TCP/IP or another LAN protocol such as IPX/SPX.

One advantage of this model is network traffic isolation and separation. SNA traffic is present only between the SNA servers and the mainframes and does not interfere with LAN traffic at each of the branch offices. This model also is preferred on those networks that already have a branch model for their IBM systems and have routers and network components already in place to handle SNA traffic over WAN links.

Centralized Deployment Model

The **centralized deployment model** positions the SNA server at the same location as the IBM host services. Clients needing access to the IBM systems connect to the SNA servers over a WAN or LAN link using TCP/IP or another supported routable protocol. One advantage of this model is centralized administration of the SNA server machines. Another advantage is the ability to provide high-speed communication between the IBM host systems and the SNA server because no WAN links are involved. One disadvantage of the centralized model is increased traffic from the client machines across the WAN and LAN links to the SNA server.

Distributed Deployment Model

The third model, the **distributed deployment model**, is a combination of the branch and centralized models. In this model, SNA servers are placed both at the branch or satellite networks and at the location of the IBM host systems. Advantages of this model are the same as for the branch and centralized models. One disadvantage of the distributed deployment model is more Windows 2000 systems are needed to run SNA Server.

SNA Integration Design

There are two factors to consider when developing a plan for integrating Windows 2000 and IBM host systems:

- WAN and LAN architecture of the network
- The type of host systems used in your environment and the location and number of clients who access these services

Depending on the results of your investigation, you can then choose the deployment model that best fits your network. If your network is an enterprise with remote locations and offices, the distributed deployment model is probably a good choice. If your current network already has in place methods and processes to handle SNA traffic over WAN and office connections, the branch deployment model may be the optimal solution.

Enhancing SNA Integration Design

In addition to the best deployment model for your network, you need to consider the impact of additional protocols on your network. With SNA servers placed at satellite offices, you may introduce SNA traffic across your WAN links. In addition to the decreased available bandwidth for other protocols, configuring SNA across WAN links may be a complicated task. In this situation, the centralized or distributed deployment model may fit your network needs.

Designing Connectivity to UNIX Servers and Clients

It is not unusual to find UNIX machines in today's networks. Quite often, UNIX systems are used to house IP-based services such as Web services, DNS, and DHCP services. In addition, software needed by an organization may exist only in a form that runs on UNIX-based systems. Also, with the increased awareness of Linux and enhancements in the installation and management of Linux systems, you might easily encounter a network with both UNIX and Linux or an environment that is moving some or all of its UNIX-based systems to Linux. Fortunately, Microsoft Windows Services for UNIX v.2 provides solutions to integrate Windows 2000 into existing UNIX and/or Linux networks.

It is very common to find UNIX systems running scripts to perform various tasks and services. Executing a script is similar in concept to a macro or batch file. Microsoft Windows Services for UNIX also allows you to migrate UNIX scripts to the Windows environment.

In the subsequent sections of this chapter, we look at the following issues as they relate to UNIX systems: file sharing, password synchronization, Telnet Server and Client, and UNIX utilities. In addition, we look at designing and enhancing a UNIX integration design.

File Sharing with Network File System (NFS)

In networks that include UNIX systems, there are usually some UNIX systems acting as servers for storing files so that all the UNIX clients have access to these files from any machine on the network. The **Network File System** (**NFS)** was developed to allow UNIX clients access to files located on a different UNIX system.

NFS is a collection of protocols and is based on the **Remote Procedure Call** (**RPC)** protocol. RPC provides a method for the exchange of messages between two machines, such

as a client and a server. On a UNIX system, to access files on a local hard drive partition, floppy disk, or CD, the storage media must be **mounted**. Mounting allows you to "place" the "contents" of the storage media into a location in the existing UNIX file system.

As an example of the use of NFS, imagine there is a directory in UNIX titled /usr/share/cdrom, which does not contain any files or subdirectories. You also have a CD-ROM that you want to use on the UNIX system. To access the CD-ROM, you would first mount the CD into a location in a file system, such as /usr/share/cdrom. After the CD is mounted, the user gains access to the contents of the CD-ROM by navigating to the directory /usr/share/cdrom. Once a storage media is mounted, users on the UNIX machine can access those files, assuming, of course, the security permissions allow the users to access the files.

Files that are located on another UNIX machine can be made accessible to the local UNIX system with NFS. With NFS, remote file systems are mounted on the local machine as if these remote files were located on the local machine. NFS provides a means to share files, and any system that supports NFS can participate in the sharing process. This allows interoperability of Windows 2000 and UNIX systems. NFS is an IP-based protocol and uses TCP as its transport protocol. Therefore, Windows 2000 systems accessing files on a UNIX system must be running TCP/IP.

Microsoft Windows Services for UNIX is a separately purchased suite of services that provides the ability to integrate and work with a UNIX environment. Here are some requirements that must be satisfied to install and run Windows Services for UNIX:

- The directory where you choose to install the software cannot contain a space in its name.
- You must be running Internet Explorer 4.01 or higher
- Any user names that contain extended characters are not supported.
- Client for NFS and Gateway for NFS cannot be installed on the same machine.
- Password synchronization and Server for NIS must be installed on a domain controller.
- The account you are logged on to when installing Microsoft Windows Services for UNIX must be the Administrator account or a member of the Administrators group.

The installation process begins by launching SETUP.EXE located on the Microsoft Windows Services for UNIX CD. There are two installation options: standard and customized. The standard installation places the components in the directory C:\SFU\. The components installed with the standard option on a Windows 2000 server are as follows:

- Server for NFS
- Server for NFS Authentication (if the Windows 2000 machine is a domain controller)

- Client for NFS
- Telnet Server
- Telnet Client
- UNIX Shell and Utilities

The customized installation allows you to specify the installation directory and service components. In addition, you can choose to install the following:

- Remote Shell Service
- CRON Service
- Gateway for NFS
- Server for PCNFS
- Server for NFS
- Password synchronization
- User Name Mapping
- ActiveState Perl
- Server for NIS

In the subsequent sections, we discuss the most commonly used features of NFS.

Gateway for NFS

The **Gateway for NFS** service is designed for Windows-based machines that need occasional access to files on a UNIX NFS system. Directories on UNIX NFS systems are configured to appear as Windows 2000 shares so that Windows machines can access files on NFS systems without installing the NFS client software on the Windows machines.

Windows systems use the Server Message Block (SMB) protocol to communicate with services and resources on other Windows systems. Gateway for NFS provides a portal on a Windows 2000 system for other Windows machines to access NFS files. The gateway tunnels all requests to and from the NFS UNIX/Linux system. Because all information between Windows and NFS travels through the gateway, access is a little slower than direct access to the NFS file system. On the other hand, you don't need to install an NFS client on each Windows machine that needs access to the NFS files. If you need frequent access to UNIX systems, we recommend that you install Client for NFS on the Windows machines.

To connect the Windows 2000 system running the gateway to the NFS system, Gateway for NFS uses a Windows account to establish a valid connection to the NFS server. This account's connection is severed only when the Windows 2000 system is shut down or when some action disconnects the share or disables the gateway. The account connection is not cleared when a user logs off and on the Windows 2000 system hosting Gateway for NFS.

Server for NFS

Server for NFS is a service that makes Windows directories appear as NFS file systems so that UNIX NFS clients can access these Windows directories. In other words, the service allows a Windows 2000 machine to act like an NFS server so that NFS clients can access the resources on the Windows 2000 system.

The NFS clients mount the Windows 2000 files on their systems as if they were files on another NFS UNIX system. If you wish to use users and groups to control access from NFS clients to Windows files, you must also install and configure Server for NFS Authentication on all controllers on the domain. If you don't use Server for NFS Authentication, all NFS users will access the Windows 2000 files as anonymous users.

In order to properly coordinate UNIX user accounts with Windows 2000 user accounts, you also must install User Name Mapping on one domain controller. If you wish to secure files on the Windows 2000 system, make sure all files that the NFS clients will access are located on NTFS volumes.

Client for NFS

Client for NFS allows users on Windows 2000 systems to access files on UNIX NFS systems. If Windows users on your network need frequent access to files on NFS systems, it is better to install Client for NFS on the Windows machines instead of using Gateway for NFS. The gateway is designed for occasional access, and access to a resource through a gateway is slower than using Client for NFS.

On Windows 2000 machines, Client for NFS adds a folder in My Network Places called NFS Network. This allows the Windows user to browse the available resources on the NFS UNIX systems. Figure 5-5 is an example of browsing a directory.

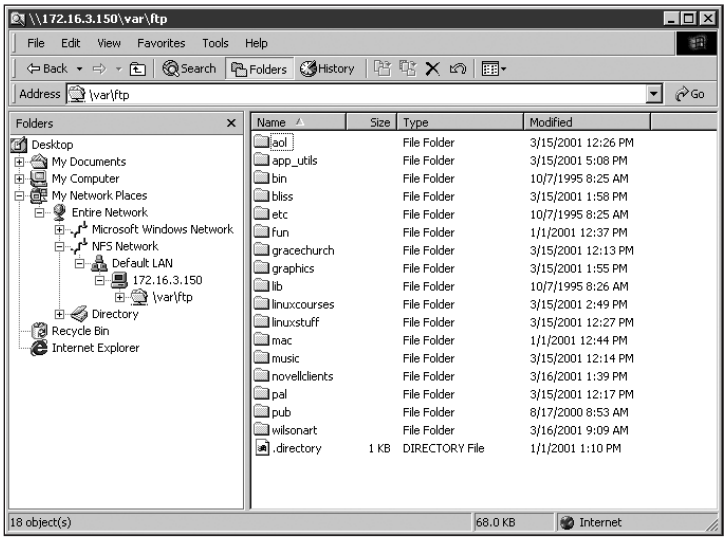

Figure 5-5 Windows 2000 system running Client for NFS and browsing a directory

Server for PCNFS

Server for PCNFS (PCNFS stands for Personal Computer Network File System, but it is usually referred to as just PCNFS) provides an authentication mechanism for users logging on to UNIX machines. The UNIX user's name and password are sent to the Server for PCNFS service, which verifies the user and returns a UID (user identifier) and GID (group identifier), which are used by the UNIX system. Server for PCNFS is included in Services for UNIX v.2 for backward compatibility for systems running version 1 of the UNIX services and for systems that cannot employ user name mapping.

Server for NIS

Network Information Service (NIS) is a network administration and naming system developed for small networks. Each host in the NIS network has a complete map of the entire network's resources, and users can access any of these resources with one account and password. NIS used to be called Yellow Pages (YP) because it provides a network lookup service. However, since the name Yellow Pages is copyrighted, the term was dropped, although you may occasionally still see it used.

Server for NIS allows a Windows 2000 domain controller to act as a master NIS server for one or more NIS domains. Server for NIS stores information about the NIS network in Active Directory. This allows a single Windows 2000 account to access both the Windows 2000 services and NIS-known resources. In addition, the administrator can manage Windows and UNIX accounts at the same time. You also can install Server for NIS on other domain controllers in the same Windows 2000 domain. This allows the other Server for NIS machines to act as NIS-subordinate servers, and the NIS data in Active Directory is automatically replicated to these NIS-subordinate servers.

Before you begin to install Server for NIS, make sure the account that is logged on is a member of the Schema Admins group. This is necessary because the Active Directory schema will be modified to handle the NIS information.

The changes to the Active Directory schema made by the Server for NIS installation are *not* reversible.

After Server for NIS is installed, you must migrate the NIS maps from the UNIX NIS servers to the Windows 2000 system running Server for NIS. This is the role of the Server for NIS Migration wizard.

You can use the Windows Service for UNIX Migration wizard to migrate maps of NIS services into Active Directory. After the NIS information is migrated, the Windows 2000 server becomes the master NIS server for the domain. Any other Windows 2000 controllers running Server for NIS become NIS-subordinate servers. In addition, the UNIX-based NIS server you migrated the maps from can be configured as a subordinate NIS server.

Password Synchronization

Password synchronization is the service that permits users to use the same synchronized password for Windows and UNIX systems. Users that need access to Windows 2000 and UNIX systems might want to use the same passwords on both systems and be able to keep them synchronized whenever there is a password change.

Password synchronization can either be one-way or two-way. With one-way synchronization, whenever the user changes his or her Windows password, the change is synchronized to his or her UNIX account of the same name. If, however, the user changes the UNIX password, the change is not sent to Windows 2000. Two-way synchronization allows a password change in either Windows 2000 or UNIX to be synchronized to the other operating system.

The password synchronization system includes configuration options. For example, you can specify user accounts and/or Windows systems that will not be synchronized, synchronize to accounts on nondomain-participating Windows 2000 servers, or synchronize accounts across an entire domain.

User Name Mapping

User Name Mapping allows you to specify user accounts and group associations between Windows 2000 and UNIX systems. This mapping can be used by Client for NFS, Gateway for NFS, and Server for NFS. User Name Mapping also allows you to map between user and group accounts that use different names in Windows and UNIX. In addition, you can create one-to-many mappings so that you can link multiple UNIX accounts to a single Windows account or link a single UNIX account to several Windows accounts.

Telnet Server and Client

Telnet is a protocol in the TCP/IP suite that permits you to log on to a remote system and use and interact with the resources your account allows. If the system you are accessing permits telnet connections and you are running a telnet client, the remote system will prompt you for an account and password. Once these are satisfied, you can work on the remote system with a command line interface as if you were actually sitting in front of the remote system.

If you want to allow telnet users to access your Windows 2000 machine through the telnet protocol, you can install the **Telnet Server** software on your Windows 2000 server. Telnet Server also has several configuration options, such as specifying the maximum number of connections, the maximum number of failed logon attempts, and setting the idle session time-out.

Telnet Client allows users on Windows systems to use telnet to log on to a remote system. Telnet Client provides a better command line interface than the plain default telnet client included with the standard Windows 2000 operating system software.

To make sure that both ends of a Telnet connection are properly interpreting the information, a standard called **Network Virtual Terminal (NVT**) is used. This allows Telnet clients from systems following NVT specifications to interact successfully with any other system supporting NVT.

When you establish a successful connection to another system by using telnet, you have set up and started a telnet session. When you establish a telnet session, you can also specify options. Probably the most common option is specifying the terminal emulation type. When you no longer need to maintain a connection to the remote machine, most terminal programs allow you to log off the remote machine, which usually ends the telnet session.

Unfortunately, telnet does not provide a great deal of security. When you log on to a remote host using telnet and you enter your password, the password is sent as plain text across the network. If you are establishing a telnet session between two Windows 2000 machines running Telnet Client and Telnet Server, you can use NTLM for authentication. This sends all logon requests to Windows 2000 domain controllers, which verify the user's identity and password.

UNIX Utilities and Korn Shell

Windows Services for UNIX includes a collection of common UNIX utilities and a shell or command line environment to execute the UNIX utilities. The command line environment included with Windows Services for UNIX is the **Korn shell**.

If you are familiar with the Korn shell or other similar shells such as BASH on a UNIX or Linux system, there are some slight syntax differences. These differences are because the Korn shell is running within the Windows environment. If the Windows 2000 system is running Telnet Server, you can configure the environment so that the Korn shell is the default shell. When users access the Windows 2000 system running Telnet Server through a telnet session, the Korn shell will be the environment they log on to.

The Korn shell provided with Windows Services for UNIX supports environment shell variables that are, for the most part, identical to a UNIX system. Similarly, many of the built-in commands in the Services for UNIX Korn shell are identical to those found on a UNIX system. The Korn shell environment in Windows 2000 also includes a large collection of utilities that are the same or similar to UNIX utilities.

Designing for UNIX Integration

Before you implement components in the Windows Services for UNIX package, you need to evaluate the types of UNIX-based services your clients are using. In addition, evaluate the location of these UNIX-based services in relation to the users. Depending on the clients and UNIX service locations, you may need to implement additional Windows 2000 systems running Windows Services for UNIX.

Enhancing a UNIX Integration Design

In networks in which users only occasionally access UNIX services, running Gateway for NFS may be a viable solution. However, if your clients regularly access UNIX-based services, consider installing Client for NFS on those Windows 2000 machines. For users running Client for NFS, you may want to make administration of user passwords easier by implementing password synchronization between Windows 2000 and UNIX. Finally, if your clients use Telnet to interact with the UNIX systems, consider using Telnet Server and/or Telnet Client.

Designing Connectivity to Macintosh Clients

Companies and organizations may include Macintosh computers in addition to Windows and other operating systems. Also, you may encounter networks that use Macintoshes for all the user machines and Windows 2000 and/or other operating systems, including Apple technologies, to provide network services. In these mixed networks, the environment may be using the TCP/IP protocol and/or the AppleTalk protocol to communicate between clients and network resources. Windows 2000 **Services for Macintosh** provides a mechanism for Windows 2000 systems to access Macintosh network services using TCP/IP or AppleTalk. Services for Macintosh also allows Macintosh systems to access Windows 2000-based services.

In the following sections, we discuss the protocols, services, and designs that you can use to successfully manage connectivity to Macintosh clients.

Protocols and Services

AppleTalk has long been a protocol used by Macintosh systems. It was developed years ago as a self-configuring protocol for small Macintosh networks. It is still supported in newer Macintosh computers in addition to TCP/IP. However, some older Macintosh equipment and services only use the AppleTalk protocol. In these situations, the AppleTalk protocol must be installed on all systems needing access to AppleTalk-dependent services.

The Services for Macintosh package includes the complete AppleTalk protocol stack and is installed automatically when you install Services for Macintosh, if AppleTalk is not already present. Services for Macintosh also includes a component called **Microsoft User Authentication Module (MS-UAM)**. MS-UAM allows the Macintosh system to log on to a Windows 2000 environment through the same security measures a Windows 2000 client encounters when logging on to a Windows 2000 system. The services and features in the Services for Macintosh package include the following:

- *File Services for Macintosh* allows Macintosh users to access files located on a Windows 2000 server.
- *Print Services for Macintosh* allows Macintosh users to print to Windows 2000-managed printers.
- *Secure logon* uses MS-UAM for logon authentication.
- *AppleTalk Phase 2* is the latest version of the AppleTalk protocol.
- *Remote access* allows Macintosh users to dial into the network over a TCP/IP connection and access both AppleTalk and TCP/IP services.

Services for Macintosh can be installed when you initially install Windows 2000 or at a later time. Installing the Macintosh services after installing Windows 2000 is done through the Add/Remove Programs applet in the Control Panel. In the Control Panel, select Add/Remove Windows Components to access the list of currently installed products and additional products. The Macintosh services are located in the Other Network File and Print Services category. There are two service categories you can choose to install: File Services for Macintosh and Print Services for Macintosh.

When File Services for Macintosh is installed, a folder titled Microsoft UAM Volume is created at the root of the NTFS volume where Windows 2000 is installed. This folder contains the MS-UAM installation files for the Macintosh clients. After the Macintosh client connects to the Windows 2000 server, it can run the software in the Microsoft UAM Volume folder. Figure 5-6 shows a Macintosh system accessing a Windows 2000 computer.

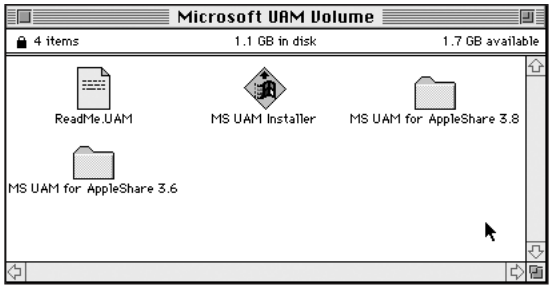

Figure 5-6 Macintosh system browsing the contents of a directory on a Windows 2000 server

Print Services for Macintosh allows a Windows 2000 system to print to an AppleTalk printer. When the service is running, the Windows 2000 machine uses the Add Printer wizard to set up printing to the AppleTalk printer. In the Add Printer wizard, you can choose to add a local printer and then choose to create a new port. When the Macintosh print services are installed, you have an AppleTalk Printing Devices port available. When this is selected, the Add Printer wizard displays a list of AppleTalk zones found on the network.

AppleTalk zones are logical groupings of AppleTalk resources, which typically use a friendly name to identify their location or usage. When you double-click the zone where the AppleTalk resource is located, the wizard displays a list of AppleTalk printers that it found in the selected zone. If the AppleTalk printer is not turned on and communicating in the AppleTalk zone, the Add Printer wizard will not find the printer.

After the AppleTalk printer is selected, you are given the option to make the printer only known to the Windows 2000 system or have it available to both AppleTalk and Windows 2000. If the network contains Macintosh systems that use the same printer through AppleTalk, then you want to make sure you do not make the AppleTalk printer exclusive to just Windows 2000. When the Add Printer wizard has completed its operations, the AppleTalk printer appears in the Windows Printers folder.

Macintosh Client Integration Designs

Before you begin adding Windows 2000 servers to a Macintosh network, you must evaluate the protocols needed by the different services. If a server or services requires AppleTalk, you will need to make sure the AppleTalk protocol is installed on the Windows 2000 servers. If there are no AppleTalk-dependent items, consider using TCP/IP in place of AppleTalk. AppleTalk was originally designed for LANs and while it is routable, AppleTalk is not a recommended protocol to go across WAN or routed LAN links.

Enhancing a Macintosh Connectivity Design

If you have a lot of Macintosh clients accessing Windows 2000 servers, you may need to support Macintosh services on all the Windows 2000 machines the users could access. In addition, if you need AppleTalk to communicate with some of your network resources, consider placing all the AppleTalk devices on the same physical network segment. This may help to reduce the amount of AppleTalk traffic competing with the TCP/IP traffic.

Chapter Summary

- In this chapter, we covered Microsoft solutions for integrating NetWare and Microsoft networks. Microsoft provides several solutions for communicating with and using NetWare technologies. There are a few core facts to remember. For instance, with Gateway Services for NetWare, a Windows 2000 server acts as a gateway to NetWare services for clients that need occasional access. For environments that access NetWare services frequently, using Client Services for NetWare on Windows 2000 systems is a good solution. In networks that are primarily NetWare and the clients are using Novell Client, running File and Print Services for NetWare on the Windows 2000 servers is the best solution. File and Print Services for NetWare makes the Windows 2000 server appear as a NetWare 3.1*x* server without any modifications to the users' systems.

- Networks that contain IBM mainframes and compatible systems can access IBM-managed data and services from Windows 2000. Microsoft SNA Server provides a communication gateway between SNA-based systems and Windows 2000. In this chapter, we covered three design suggestions for placement of SNA servers in your existing IBM host system network: branch deployment, centralized deployment, and distributed deployment.
- Microsoft also provides a solution for networks that have UNIX systems. Microsoft Windows Services for UNIX includes several components to access UNIX-managed resources and for UNIX clients to access data on Windows 2000 servers. There are critical facts that you should remember about this technology. For instance, Gateway for NFS is designed for occasional access to an NFS system without the need to install a client software piece on the Windows 2000 systems. Server for NFS enables a Windows 2000 server's directories to appear as NFS-shared directories. Client for NFS running on Windows 2000 systems allows users access to directories on NFS systems. A Windows 2000 server can also be configured to operate as a NIS server. With the Password Synchronization tool, you can synchronize password changes between Windows 2000 and UNIX systems. The services for UNIX also include the Korn shell, many of the common UNIX utilities, and an enhanced Telnet server and client.
- In the last portion of this chapter, we covered Services for Macintosh, which permits Macintosh systems access to Windows 2000 directories and services. In addition, Services for Macintosh Windows 2000 allows users to access AppleTalk-managed services such as printing.

Key Terms

Active Directory (AD) — Directory service developed by Microsoft.

bindery — The name given to the database used by NetWare 3.*x* to hold user accounts and related information.

branch deployment model — SNA design model where SNA servers are placed at satellite or branch offices.

centralized deployment model — SNA design model where SNA servers are located at the same location as the IBM systems.

Client for NFS — Allows Windows 2000 system users to access files on UNIX NFS systems.

Client Services for NetWare (CSNW) — Microsoft's version of a client used to access NetWare systems.

context — Name of the container in an NDS database where the object in question resides.

distributed deployment model — SNA design model that is a combination of the branch and centralized deployment models.

File and Print Services for NetWare (**FPNW**) — One of the Windows 2000 services for NetWare that emulates a NetWare 3.*x* server.

gateway — Software that converts one protocol to another protocol.

Gateway for NFS — Directories on UNIX NFS systems that appear as Windows 2000 shares.

Gateway Services for NetWare (GSNW) — Software that runs on a Windows 2000 server and allows Microsoft clients access to Novell-managed services.

Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX) — A communication protocol developed by Novell that is necessary for proper communication between NetWare 2.*x*, 3.*x*, and 4.*x* servers.

Korn shell — One type of command line interface environment used on UNIX systems.

login scripts — Commands and/or settings executed when an account logs into the NetWare environment.

Microsoft Directory Synchronization Services (**MSDSS**) — Collection of tools for integrating and/or migrating NDS and AD.

Microsoft SNA Server — Service that provides connectivity between IBM mainframes and Windows 2000.

Microsoft User Authentication Module (MS-UAM) — Allows the Macintosh system to log on to a Windows 2000 environment through the same security measures a Windows 2000 client encounters when logging on to a Windows 2000 system.

mounted — UNIX term referring to online accessible storage devices.

Network File System (NFS) — Service on a UNIX machine for accessing files remotely.

Network Virtual Terminal (NVT) — A protocol used by Telnet sessions so that both ends of the connection can understand each other properly.

Novell Client for Windows NT/2000 — Client software developed by Novell to access NetWare-managed resources.

Novell Directory Services (NDS) — A directory service developed by Novell and used in NetWare 4.*x* and higher.

NTGATEWAY — A NetWare group required to install and use Gateway Services for NetWare.

NWLink — Microsoft's implementation of Novell's IPX/SPX protocol.

password synchronization — Permits users to use the same synchronized password for Windows and UNIX systems.

publisher — Term used by Microsoft to refer to Active Directory when migrating directory data from NetWare to Windows 2000.

Remote Procedure Call (RPC) — Protocol used to exchange messages between machines.

SAP Agent — Service running on the Windows 2000 system responding to queries from clients such as Get Nearest Server.

Server for NFS — Windows directories appear as NFS file systems.

Server for NIS — Allows a Windows 2000 server to operate as a NIS server and to integrate with other NIS servers and domains.

Server for PCNFS — Allows Windows systems running NFS Client to authenticate to UNIX systems.

Service Advertising Protocol (SAP) — Used by IPX/SPX services to make known their identity and services.

Services for Macintosh — Provides a mechanism for Windows 2000 systems to access Macintosh network services using TCP/IP or AppleTalk.

Services for NetWare (SFN) v.5 — Designed for integrating Windows 2000 server systems into an existing NetWare environment.

session — A logical connection between Active Directory and Novell Directory Services.

subscriber — Term used by Microsoft to refer to the NetWare system when migrating files from NetWare to Windows 2000.

Systems Network Architecture (SNA) — Communication protocol developed by IBM.

Telnet Client — Connects to ands run applications on a Telnet server.

Telnet Server — Allows systems using Telnet access to the Windows 2000 server.

Transmission Control Protocol/Internet Protocol (TCP/IP) — Communication protocol used on the Internet. It is commonly found on large networks.

tree — Name of an NDS database.

Review Questions

1. What protocol is required by Gateway Services for NetWare? (Choose all that apply.)
   a. TCP/IP
   b. SAP
   c. NWLink
   d. SNA
2. What is the main function of NFS?
3. To access a Novell NDS network, what two parameters must be specified in Gateway or Client Services for NetWare?
4. The purpose of MS-UAM is to allow clear text information to pass between the Macintosh and the Windows 2000 system. True or False?
5. What are the requirements of the user account specified in the GSNW settings?
6. Explain what MSDSS does.
7. What is the purpose of the Microsoft File Migration utility? (Choose all that apply.)
   a. migrate files from NetWare systems to Windows 2000 systems
   b. migrate files from older Windows NT systems to Windows 2000 systems
   c. migrate files from Macintosh systems to Windows 2000 systems
   d. migrate files from Windows 2000 systems to NetWare systems

8. What is the function of File and Print Services for NetWare? (Choose all that apply.)
   a. makes a NetWare server appear as a Windows 2000 server on the network
   b. makes an AppleTalk printer accessible to NetWare users in a Windows 2000 network
   c. makes a Windows 2000 server appear as a NetWare server on the network
   d. allows NetWare users in a Windows 2000 network to print to a NetWare-managed printer
9. What are some of the options you can specify in the GSNW settings?
10. In what types of networks would Server for NFS fit the best?
11. Client Services for NetWare is a solution recommended for which of the following? (Choose all that apply.)
    a. users needing occasional access to NetWare host services
    b. users needing access to the NetWare network using only TCP/IP
    c. users needing frequent access to NetWare host services
    d. users needing to install services on a NetWare server
12. What additional products must be installed on the GSNW machine for a user to log on to the machine running GSNW?
13. What additional products must be installed to make MSDSS function?
14. GSNW is installed through the Add/Remove Programs interface. True or False?
15. List the services SNA Server provides.
16. The Directory Synchronization tool allows you to synchronize Windows 2000 systems with bindery-based NetWare systems. True or False?
17. Which of the following groups is required by GSNW? (Choose all that apply.)
    a. GSNWGroup
    b. NTGATEWAY
    c. W2KGATEWAY
    d. MSDSSGroup
18. What must be done to NDS in order to install two-way synchronization?
19. The branch deployment model places the SNA and Windows 2000 systems in satellite offices. True or False?
20. What is the Korn shell? (Choose all that apply.)
    a. a command line interface used in UNIX systems
    b. a troubleshooting tool for checking UNIX system logs
    c. the Kernel Object Reference Notify protocol used on UNIX networks
    d. a graphical user interface (GUI) used on UNIX systems

21. Explain how GSNW works.
22. In the Microsoft File Migration utility, the Windows 2000 system is the subscriber. True or False?
23. What services must be present for FPNW to function?
24. Describe the distributed deployment model.
25. What protocols can be used by Macintosh systems to access Windows 2000 directories?
26. Describe how Gateway for NFS functions.

HANDS-ON PROJECTS

Project 5-1 Gateway Services for NetWare

For this project, you will need a computer running Windows 2000 Server and access to a NetWare 4.*x* or 5.*x* server.

1. If your server is not powered up, power it up now.
2. Press **Control+Alt+Delete** to display the Log On to Windows dialog box.
3. In the Password box, type **password** (if this does not work, ask your instructor for the password.)
4. When the desktop appears, click the **Start** button.
5. Point to **Settings**, click **Network and Dial-up Connections**, right-click **Local Area Connection**, and choose **Properties**.
6. Click the **Install** button.
7. Click **Client**, if necessary, and then click **Add**.
8. Select **Gateway (and Client) Services for NetWare**.
9. Click **OK**.
10. Type **NetWare-Tree** in the Tree text box and **.austin.tx.com** in the Context text box. (The information that you use in this step may differ. Consult with your instructor.)
11. Click **OK** and when the machine says to reboot, reboot your Windows 2000 server.
12. Press **Control+Alt+Delete** to display the Log On to Windows dialog box.
13. In the Password box, type **password** (if this does not work, ask your instructor for the password).
14. When the desktop appears, click the **Start** button.
15. Point to **Settings**, click **Control Panel**, and double-click the **GSNW** icon.
16. Click **Gateway** and then select **Enable Gateway**.

17. Enter the name of the NetWare user account in the Gateway Account text box. Ask your instructor for the name of the user account.
18. Enter the password in the Password and Confirm Password text boxes. Ask your instructor for the user account's password.
19. Click **OK** twice.
20. Reboot your machine and log on as the administrator.
21. Verify that you are connected to the NetWare server by browsing the NetWare server contents. If you can see directories and files, then you have a connection.
22. When you have finished, close all open windows.

Project 5-2 Client for NFS

For this project, you will need a computer that is running Windows 2000 and have access to a Linux system. You also will need the Windows Services for Unix v.2 CD.

1. If your server is not powered up, power it up now.
2. Press **Control+Alt+Delete** to display the Log On to Windows dialog box.
3. In the Password box, type **password** (if this does not work, ask your instructor for the password).
4. When the desktop appears, browse the contents of the Windows Services for the UNIX CD.
5. Double-click **SETUP.EXE** found at the root of the UNIX CD.
6. Click the **Next** button.
7. Enter the user name, organization and Product Key, if necessary, and click **Next**.
8. Click the **I accept the agreement** option button, and then click the **Next** button.
9. Select **Customized installation** and click the **Next** button.
10. Navigate through the options and make sure Client for NFS is selected, and then click the **Next** button.
11. Click **Next** on the User Name Mapping screen.
12. Accept the default installation location, click the **Next** button, and then click **Finish**.
13. Reboot your computer and log in as the administrator.
14. Open Windows Explorer and expand the **Entire Network** icon.
15. Expand **NFS Network**, expand **Default LAN**, and expand the computer icon below Default LAN.
16. Select the folder below the computer icon to view the contents of the folder located on the Linux system.
17. When you have finished, close all windows.

Project 5-3 Macintosh Services

For this project, you will need a computer that is running Windows 2000.

1. If your server is not powered up, power it up now.
2. Press **Control+Alt+Delete** to display the security dialog box titled Log On to Windows.
3. In the Password box, type **password** (if this does not work, ask your instructor for the password).
4. Press **Return**.
5. When the desktop appears, click the **Start** button.
6. Point to **Settings**, click **Control Panel**, and then double-click **Add/Remove Programs**.
7. In Add/Remove Programs window, click **Add/Remove Windows Components**.
8. In the Components section of the Windows Components wizard, use the scroll bar to scroll down the component list until the words Networking Services appear.
9. Click the words **Other Network File and Print Services** (do not click the check box), and then click the **Details** button on the right below the Components box.
10. In the Other Network File and Print Services window, click the **File Services for Macintosh** and **Print Services for Macintosh** check boxes, and then click **OK**.
11. When you are returned to the Windows Components wizard, click **Next**, and then click **Finish**.
12. Close all open windows on the desktop.

Project 5-4 Using Telnet

For this project, you will need a computer running Windows 2000 Server with Microsoft Windows Services for UNIX v.2 installed, which includes the Telnet Server and Client components. You will also need to ask the instructor for a Linux machine's IP number, an account name, and a password to use. (Linux is a flavor of UNIX.)

1. If your server is not powered up, power it up now.
2. Press **Control+Alt+Delete** to display the Security Dialog box titled Log On to Windows.
3. In the Password box, type **password** (if this does not work, ask your instructor for the password).
4. When the desktop appears, click the **Start** button.
5. Point to **Programs**, point to **Windows Services for UNIX**, and choose **Telnet Client**.
6. To see the available commands in the Telnet client, type **help**, and press **Enter**.

7. Ask your instructor for the Linux machine's IP number, an account name, and a password to use.
8. Type **open <*IP number*>**, where <*IP number*> is the IP number of the Linux machine. Press **Enter**.
9. At the login prompt, type the Linux account name and press **Enter**.
10. At the password prompt, type the Linux account's password and press **Enter**.
11. To verify your connection on the Linux system, type **w** and press **Enter**. You should see the Linux account name and IP number of your Windows 2000 system listed.
12. To log off the Linux system, type **exit** and press **Enter**.
13. At the Press any key to continue prompt, press any key.
14. To exit Telnet Client, type **quit** and press **Enter**.
15. When you have finished, close all open windows.

Project 5-5 Configuring GSNW

For this project, you will need a computer that is running Windows 2000, the GSNW configured for access to a NetWare server, and a NetWare 4.*x* or 5.*x* server. You also will need the name of a NetWare server.

1. If your server is not powered up, power it up now.
2. Press **Control+Alt+Delete** to display the security dialog box titled Log On to Windows.
3. In the Password box, type **password** (if this does not work, ask your instructor for the password).
4. Ask your instructor for the name of the NetWare server.
5. When the desktop appears, click the **Start** button.
6. Point to **Settings** and choose **Control Panel**.
7. Double-click the **GSNW Control Panel** applet.
8. Click the **Gateway** button.
9. Click the **Add** button.
10. Type **NWPublic** in the Share Name text box.
11. In the Network Path text box, type the following, where **<***NetWare Server Name***>** is the name of the NetWare server given to you by your instructor:

    \\<*NetWare Server Name*>sys\public
12. Type **NetWare Public Folder** in the Comment text box.
13. In the Use Drive text box, choose **N:** as the drive letter (or whatever letter your instructor indicates).
14. Click the **OK** button.

15. Click the **OK** button in the Configure Gateway window.
16. Click the **OK** button in the Gateway Services for NetWare window.
17. Close the Control Panel window.
18. Explore My Computer and you will see a listing for public on <NetWare Server Name>\sys (N:).
19. Double-click the drive **N:** and browse the contents of the Public folder on the NetWare server.
20. When you have finished, close all open windows.

Project 5-6 Configuring to Print to an AppleTalk Printer

For this project, you will need a computer that is running Windows 2000 and a LaserWriter printer attached to an AppleTalk network.

1. If your server is not powered up, power it up now.
2. Press **Control+Alt+Delete** to display the security dialog box titled Log On to Windows.
3. In the Password box, type **password** (if this does not work, ask your instructor for the password).
4. Press **Return**.
5. When the desktop appears, click the **Start** button.
6. Point to **Settings** and choose **Printers**.
7. Double-click **Add Printer**.
8. Click **Next** in the Add Printer wizard window.
9. Verify that the **Local printer** option button is selected and that the **Automatically detect and install my Plug and Play printer** check box is not selected.
10. Click the **Next** button.
11. Select the **Create a new port:** button.
12. Verify the type is set to AppleTalk Printing Devices.
13. Click the **Next** button.
14. Double-click the name of the AppleTalk Printing Devices specified by your instructor.
15. Select the name of the AppleTalk printer specified by your instructor.
16. Click the **OK** button.
17. In the Windows dialog box that appears asking if you want to capture the AppleTalk device, choose **No**.
18. In the Manufacturers list, select **Apple**, and under the Printers list, choose the type of printer specified by your instructor.

19. Click the **Next** button.
20. Accept the default name for the printer and click the **Next** button.
21. Change the Share as name to **Apple Printer** and click the **Next** button.
22. Click **Yes** in the dialog box confirming the name of the share.
23. Click the **Next** button.
24. Choose **Yes** to print a test page, and then click **Next**.
25. Click the **Finish** button.
26. Click **OK** in the test page window.
27. When you have finished, close all open windows.

CASE PROJECTS

Case 5-1 Design a NetWare Integration Plan

Desert Snow, a manufacturer of chocolate candies, is a midsize company located in central Kansas. They have been using Windows NT 4.0 since 1998 to support 423 employees. Recently, three NetWare 5.*x* servers were installed to manage the company's printers and to store files used by the employees. Design an integration plan that would allow the users access to the NetWare servers in an efficient manner.

Case 5-2 Design an SNA Integration Plan

Magnum Widgets, a large manufacturer of office plastic products, has been using IBM mainframes and dedicated terminals to interact with the mainframes. All of the mainframes are housed at Magnum Widgets' main location in Austin, Texas. The majority of employees are located in ten different cities around the United States and communicate with the central office over ISDN lines. Recently, Magnum Widgets purchased Windows 2000 systems to replace the dedicated terminals. Design a solution for the new Windows 2000 machines to efficiently access the data on the IBM mainframes.

Case 5-3 Design a UNIX Integration Plan

Accurate Accounting has been using UNIX servers and workstations to house and interact with their client database. Some employees will be receiving Windows 2000 machines and will need to access the information in the UNIX servers. Design a solution for the new Windows 2000 users to work with the data on the UNIX servers.

Case 5-4 Design a Macintosh Integration Plan

South Pole Digital Music uses Macintosh systems to produce a wide range of music DVDs. They have recently replaced their AppleShare servers with Windows 2000 servers. Design a solution to allow the Macintosh users access to the Windows 2000 server using the same security a Windows 2000 machine accessing a Windows 2000 server would encounter.